LOUISIANA TECHNOLOGY INNOVATION FUND
Revised 8/7/2003

I PROJECT TITLE

Active Directory

II PROJECT LEADER

Rex McDonald
Department of Public Safety & Corrections
Data Center
8001 Independence Blvd.
225.925.6226
225.925.4019
rmcdonal@dps.state.la.us

III EXECUTIVE SUMMARY

The Department of Public Safety is submitting this request for a project that will provide for the statewide implementation of Active Directory. This will include planning, designing architecture, developing policies and procedures, and assisting with the deployment (where required) of a solid Windows 2000 infrastructure based on Active Directory implementation best practices. This will enable the state of Louisiana to achieve their business objectives as outlined in the State IT Master Plan. (http://www.state.la.us/oit/docs/IT_Master_Plan_041102.pdf) . The architecture, implementation plan, and policies and procedures developed will be used as a road map when assisting agencies joining the single state wide Active Directory (AD).

Active Directory presents organizations with a directory service designed for distributed computing environments. AD allows organizations to centrally manage and share information about network resources and users. AD acts as the central authority for network security and provides comprehensive directory services. AD is a consolidation point for isolating, migrating, centrally managing, and reducing the number of required directories thereby reducing administrative overhead.

This project will cost $300,000. It will begin as soon as the contract is awarded and the project will be completed in 18 months.

IV DESCRIPTION OF THE PROJECT

This project will give state agencies the advantages of the collaborative, security, and cost benefits of a global infrastructure provided by Active Directory. Active Directory centrally manages Windows users, clients, and servers through a single consistent management interface, reducing redundancy and maintenance costs.

The goal of this project is to provide for the smooth transition of state agencies into the la.gov forest. This transition can only be achieved through careful planning and implementation. In addition to establishing policies that reflect the best practices, all aspects of the la.gov domain architecture must be must be meticulously planned and documented. Active Directory's benefits include manageability, security, and interoperability.

Active Directory provides for central management of Windows users, clients, and servers through a single consistent management interface, thereby reducing redundancy and maintenance costs. AD provides

administrators with automatic software distribution and maintenance, centralized desktop-configuration management, and remote operating system installation.

Active Directory reduces the costs and time associated with upgrades and new installs. Agencies can reap the benefits of the latest software applications without the delay associated with individual installs. AD provides a directory-enabled application (DEA) platform which enables applications to make use of the directory for automating aspects of their installation, distribution, and maintenance. Active Directory makes it easier for users to share information with one another, reducing redundancy. Users on the network can publish important information in the directory so other users can easily find it. Active Directory, combined with hardware and software support from Cisco Systems, introduces a directory-enabled networking (DEN) platform that allows administrators to allocate network bandwidth and quality of service to users based on priority.

Group Policy allows administrators to define and control the policies governing groups of computers and users within their organization. Administrators can set group policy for any of the sites, domains, or organizational units in Active Directory. They can also filter its effect by using membership in security groups. Once set, the system maintains group policy without need for further intervention. The Global Catalog holds all objects from all domains in the Windows 2000 Server directory, together with a subset of each object's properties. Designed for high performance, the Global Catalog lets users search by selected attributes to find an object easily, regardless of where it is in the tree.

B. Use of Innovative Technology

For end users, the IntelliMirror component provides location independence by making user-specific desktop settings, application data and documents available from any machine on the network. Active Directory lets administrators automatically distribute applications to users based on their role in the company. For example, all accountants can automatically receive spreadsheet software.

The development of directory-enabled applications and the administration of distributed systems are also improved. Developers and administrators use this single set of interfaces to manage the resources in a directory service, no matter which network environment contains the resource. ADSI supports interfaces for ActiveX/COM, Lightweight Directory Access Protocol (LDAP), MAPI and Java (JADSI). Windows 2000 lets administrators delegate a selected set of administrative privileges to appropriate individuals within an agency and specify the rights they have over different containers (collections of objects) and objects in the directory.

Replication and redundancy are keys to Active Directory's reliability. With multi-master replication, the changes made to any one domain controller will also be made to all the other domain controllers in the same domain. Even if individual domain controllers are unavailable, multi-master replication assures that the directory is available for changes 100 percent of the time. In addition, by providing multiple copies of the directory across multiple servers, the Windows 2000 Server directory automatically optimizes the use of replication bandwidth across WAN links.

Fewer trusts relationships promote manageability, security, and reliability. Transitive trust agreements greatly reduce the number of trust relationships to manage between Windows domains. The Global Catalog enforces object and attribute-level security for detailed control of access to information stored in the directory. In Windows 2000, there are no restrictions on security groups that span domain partitions. This means that groups can be managed centrally. Consistent interpretation of access control lists (ACLs) through LDAP ensures interoperability for secure extranets and e-commerce applications.

C. Multi-agency Application or Portability to Other Agencies

This project will affect all state agencies. The Division of Administration, the Department of Education, and the Department of Public Safety have already joined la.gov. As other agencies join, they too will reap the benefits of this project. The deployment assistance, planning, architectural design, policies and procedures that result from this project will ensure that each agency will achieve the best possible result.

D. Benchmarking Partners and/or Best Practice References

The National Association of State Chief Information Officers publishes their agreed upon best practices. Many of them are applicable to this project. They include the following:

Ensuring collaboration among state agencies to maximize the use of technology.

Consolidation across departmental lines of infrastructure and related service.

Demanding interoperability for government communication systems.

Cross-agency policy implementation and project management support.

The NASCIO states that these practices result from a growing emphasis on greater consistency in the use of IT solutions and the need to involve multiple organizations that previously focused solely on their own domains.

Active Directory is being used with success not only by private industry but also by state and federal agencies. Examples include Pennsylvania, the US Senate, and the Department of the Interior.

Pennsylvania had 40,000 unique desktops in 47 agencies with over 100 domains, and many different email systems on six different platforms. Now the entire state is united on a common Microsoft® platform with Windows® 2000 Server Active Directory™ service centralizing management across the entire organization. The results: The Commonwealth saved $9.2 million over the three years of implementation and lowered the total cost of ownership for e-mail and collaboration by $9 million. A more detailed account of Pennsylvania's experience can be found at
http://www.microsoft.com/windows2000/server/evaluation/casestudies/cop.asp

The current CIO and point of contact in Pennsylvania is **Arthur Stephens**
CIO/Deputy Secretary for Information Technology
Commonwealth Technology Center
Phone: (717) 787-5440
Fax: (717) 787-4523
Year Appointed: 2003

Another example of a government agency implementing Active Directory is the United States Senate. The Senate sergeant at arms has named the first chief information officer for the chamber, Greg Hanson. One of his priorities is to move a number of Senate offices to create a Senate wide Active Directory.
http://www.gcn.com/vol1_no1/daily-updates/22570-1.html

The Department of the Interior is currently using Active Directory.
Their CIO is Mr**. W. Hord Tipton**
1849 C Street, NW
Washington, DC 20240

hord_tipton@ios.doi.gov
Phone: 202-208-6194

E. Long-range Planning

The State IT Master Plan states goals that include establishment of enterprise architecture, centralization, enterprise delivery of application and desktop services. The plan specifically targets 2003 for the implementation of a Common Directory. Each of these goals will be significantly furthered by the successful implementation of a Statewide Active Directory.

These larger goals are reflected in the Department of Public Safety's long range plan.

Strategy II.1.16 Calls for the implementation of a Domain environment.
Strategy II.1.17 Calls for the implementation of Active Directory.

This project also fits with the broader goal of using technology in a cost effective way to better serve our customer/citizens in all areas.

F. Performance Goal

Develop implementation plan

Design architecture

Develop policies and procedures

Assist with deployment

Organizations continue normal business operations while migrating to Statewide Active Directory.

Minimal modifications to the existing network infrastructure.

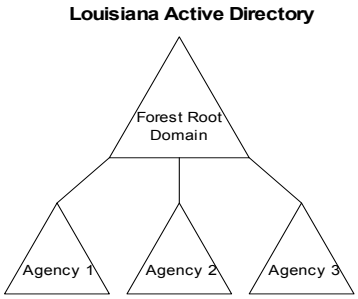
Existing user accounts and resource permissions to be migrated.

Migration of services and applications running on existing servers.

G. Technical Approach

1. Technical description. **Forest Structure:**

Single Forest with multiple Domains. Domain ownership is delegated to each agency.



Organization
Active Directory is tied tightly to the DNS structure, and follows the DNS hierarchy for domains. Active Directory introduces the concept of the "forest" of domain trees, which share certain things in common, but remain separate domains for administrative purposes. Active Directory is created hierarchically, allowing for better organization and ease of use at the resource level, too. No longer are all of the users and groups organized in a single list, as in User Manager for NT4 Domains. Sub-containers, called Organizational Units (OUs) can be created, so that, for instance, all of the user, groups, printers, etc., for a single geographic location can be placed together, making them easier to find and administer.

Centralized Management/Control
With a single set of management tools, the entire Directory can be managed from a single location. AD also allows for much more granular delegation of rights, so that certain administrative tasks can be delegated, while still retaining a secure environment.

Single Sign-on
Active Directory brings us that much closer to the administrator's dream of single sign-on for users. This means only one login name to remember, one password to remember and change, and so on. As more applications become AD-enabled, this dream becomes a reality. Imagine, for instance, when an accountant leaves the company, disabling a single AD account, rather than disabling the NT domain account, the AP/AR software account, the Payroll software account, etc.

2. *Interoperability*. Active Directory does offer the option of running in mixed mode to allow NT Servers to coexist with 2000 servers. This is called mixed mode. We have chosen not to use mixed mode but instead to use native mode which requires that all servers be running Windows 2000. Major advantages of native mode include support for universal groups, nested groups, and transitive trust relationships. One of the biggest drawbacks of mixed mode is that AD's scalability is limited to 40MB because the PDC emulator replicates changes to NT domain controllers that inherit limited scalability by design. By default, Win2K domain controllers establish an automatic two-way Kerberos trust relationship with all other domain controllers in a domain. Because NT domain controllers don't understand Kerberos transitive trusts, you have to establish explicit (manual) one-way trusts between domains to authenticate users from other domains.

3. S*calability.* One of the most apparent advantages to using Active Directory over using either NT4 Domains or a Workgroup model is that Active Directory can accommodate size. In a workgroup environment, a user account with password has to exist on each computer with shared resources. If you have three servers and ten users, that means creating thirty user accounts total, and each user would have to remember or synchronize three passwords each. AD also overcomes the limitations and work-around for large enterprises using NT4 domains. Active Directory domains can contain many more groups and users, rendering the Account domains, and Resource domains from NT4 obsolete

4. Maintaining the System. Each agency will be responsible for maintaining their own domain. Overall maintenance of la.gov will be the responsibility of DPS personnel.

Roles and Responsibilities of the Forest Owner – (Department of Public Safety)

Role	Responsibilities
Service owner for domain controllers in the forest root domain	Manages domain controller configuration throughout the forest to manage replication issues.
Administrative owner for data in the forest root domain	Manages and Controls membership of Domain Admins, Enterprise Admins, and Schema Admins security groups in the forest root domain.
Administrative oversight of all domain data	Through the Enterprise Admins group, the forest owner can correct errors anywhere in the directory. Enterprise Admins administrative access to non-root domains is required.
Administrative owner of the schema	Schema Admins Committee: □ Sets policy for schema extensions □ Sets process for schema extensions □ Controls who extends the schema
Administrative (and policy) owner of the configuration	Through Enterprise Admins: □ Acts as gatekeeper for new domains in the forest □ Administrative owner of site topology

Domain Owner's Roles and Responsibilities – (Each Participating Agency)

Area of responsibility	Associated tasks
Managing domain controller operations	□ Creating and removing domain controllers. □ Domain controller health monitoring. □ Managing services running on domain controllers. □ Backing up and restoring.
Configuring domain-wide settings	□ Creating domain and domain user account policies such as password, Kerberos, and account lockout according to OIT defined standards.
Delegating data-level administration	□ Creating OUs and delegating administration. □ Repairing problems in the OU structure that OU owners do not have sufficient access rights to fix.
Managing External trusts	□ Creating trust links with domains outside of the forest.

G. Implementation Approach

The approach taken for producing the enterprise architecture is based on the Microsoft Solutions Framework (MSF). Planning, testing and implementation will proceed as follows.

- Windows 2000 Architecture
  - Forest Structure
    - Forest Design Recommendation
  - Domain Structure
    - Recommendations for Domain Design
  - Organizational Unit Structure
    - Recommended OU design
  - Active Directory Site Structure
    - Site Design Criteria
    - Recommendation for Site Design
  - Active Directory Server Types and Roles
    - FSMO Servers
    - Global Catalog Servers
    - Domain Controllers

- Domain Name System (DNS) Design
  - Existing DNS Structure
  - DNS Design Goals and Requirements
  - Recommended DNS Design

- WINS Architecture
  - Current WINS Infrastructure
  - Recommended WINS design

- Other Services
  - DHCP Configuration
  - Time Service Configuration
  - Trust Configuration

- Naming Standards
  - Illegal Characters
  - Organizational Unit
  - Servers
  - Printers
  - Logon and User Principal Naming
  - Groups
  - Group Policies

- Management Architecture
  - Schema Management
  - Administrative Roles, Permissions, Scope, Prerequisites, Logon Requirements
  - Support Tools and Methods

- Group Policy
  - Group Policy Application
  - Applying Group Policy
  - Group Policy Objects
  - GPO Domain Password Settings
  - Logon Banners

I. Assessment of Risks

This project is not without risks. One risk is that if implementation and deployment are not adequately planned and properly implemented, problems will be magnified across the domain. These risks will be mitigated with architectural design, development of policies and procedures, planned implementation, and deployment assistance. This project will save agencies from duplicating research and planning as well as ensuring consistency across the domain.

Another risk is that individual agencies may not have the funding necessary for the licenses and upgrades required to join Statewide Active Directory. The benefits of a Statewide Directory Service are directly tied to agency participation. The greatest benefit will be derived when all agencies join.

J. Integration with Existing Technologies

This project will build upon the infrastructure that is already being used by the Division of Administration, Department of Education, and the Department of Public Safety. The Department of Environmental Quality is scheduled to become the next member.

As discussed previously in the interoperability portion of this document, we have chosen to operate in native mode, not mixed mode. This will require that NT servers be upgraded to 2000 before they can be integrated into the domain. This choice was made based on the factors outlined above in the interoperability section.

K. Project Budget and Costs

PROFESSIONAL SERVICES

Systems Development Contract. Professional services will be required to asses existing architecture and recommend necessary changes. Policies and procedures and an implementation plan will be developed based on these assessments. It is estimated that 3,000 hours of consulting services at $100/hr will be required.

Cost Summary:

Item	Quantity	Unit Price	Total
Professional Services	3,000	$100/hr	$300,000
Total			**$300,000**

V FUNDING REQUESTED

LTIF will be the only source of funding**.**

VI COST/BENEFIT ANALYSIS

	Expenditure Increase (Decrease)		
STATE COSTS	**2003-2004**	**2004-2005**	**2005-2006**
Professional Services			
Designing Architecture	500 hrs		
Planning	500 hrs		
Developing policies/procedure		1,000 hrs	
Assisting with deployment		1,000 hrs	50,000
Total State Exp.	**100,000**	**200,000**	**50,000**

MEANS OF FINANCING FOR ABOVE EXPENDITURES

FISCAL YEAR	**LTIF**	**New Active Directory member agencies.**
2003-04	**100,000**	
2004-05	**200,000**	
2005-06		**50,000**

Narrative Explanation of Expenditure Impact

1) Implementation Costs will include $200,000 for designing architecture, planning, and developing policies/procedures over a period of 18 months. The remaining $100,000 will be spent assisting other agencies in joining Statewide Active Directory. This will occur during the final 6 months of the project. We estimate that 5 agencies will be ready to join in FY 2005-2006. We estimate that upon completion of this project we will be able to provide agencies with the assistance necessary to join the domain at a cost per agency of $10,000. Without this project, the planning and architectural design will have to be duplicated within each agency; greatly increasing the total cost to achieve the business objective of a single directory as outlined in the State IT Master Plan.

2) Source of Funds. The initial 18 month project will be funded by the Louisiana Technology Fund. In addition, the Department of Public Safety will contribute existing IT staff, facilities, and equipment. Subsequent costs will be funded by member agencies based upon a cost model to be developed.